SWATTING PREVENTION AND RESPONSE GUIDANCE FOR ELECTION WORKERS AND LAW ENFORCEMENT

OVERVIEW

Swatting is a term used to describe criminal activity by an individual or group who knowingly provides false information to law enforcement suggesting that a serious threat exists at a particular location so that law enforcement responds with tactical units, or what's commonly known as a SWAT (special weapons and tactics) team. This dangerous tactic places the targeted individual or location and law enforcement at risk and pulls critical first responder resources away from actual emergencies. In late 2023 and early 2024, there were multiple swatting incidents specifically targeting election workers[1]. This guidance document provides an overview of swatting and recommended practices for preventing and responding to swatting incidents for both election workers as well as law enforcement.

UNDERSTANDING SWATTING

Both foreign and domestic actors use swatting as a method to harass or intimidate individuals and businesses, including U.S. government officials, faith-based institutions, schools, journalists, company executives, and celebrities. They may also seek to disrupt critical infrastructure operations, induce fear or chaos, divert law enforcement from other crimes or emergencies, or simply gain attention or notoriety. Similar to doxing and phishing tactics, malicious actors engaging in swatting often rely on open-source information or social engineering techniques to uncover information about their target. Swatters will place calls to emergency lines like 9-1-1 or nonemergency lines of law enforcement agencies and falsely report a violent emergency situation requiring an immediate response, such as an active shooter, bomb threat, home invasion, or hostage situation, attempting to muster the largest emergency response possible. They may even use technology to make it appear as if the emergency call is coming from the victim's phone number[2]. Swatters will often present a plausible scenario and will sometimes include personal information gathered online about the victim to make the call more believable.

Confusion on the part of the target(s) and responding officers has tragically resulted in fatal consequences. Swatting also diverts limited emergency response resources away from real emergencies, indirectly causing harm to victims beyond the specific target(s).

REDUCING RISK TO ELECTION WORKERS AND FACILITIES

Although swatting incidents to date have targeted homes of election officials, malicious actors could expand this tactic to target other facilities in order to disrupt election operations. This could include swatting attempts to disrupt election operations at polling places, election offices, or central count facilities. Law enforcement and election workers can take steps to reduce the risks from swatting. To help prevent potential swatting incidents, election officials should **partner with local law enforcement and emergency responders** to share, in accordance with your organization's privacy policy, the names and addresses of election workers and election-related locations and collaborate on mitigation strategies. Election workers are also encouraged to implement best practices for **reducing the availability of their personally identifiable information online[3].**

---

[1] "Election Officials' homes 'swatted' as presidential race heats up." https://www.cnn.com/2024/03/13/politics/swatting-election-officials-invs/index.html
[2] Caller ID Spoofing | Federal Communications Commission (fcc.gov)
[3] CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure | CISA

Swatting Prevention: What to do to Mitigate Risk from a Swatting Incident

- **Establish Relationships between Election Offices, Law Enforcement and Emergency Responders.**
  - Law enforcement should consider contacting their local election workers to understand their concerns and needs.
  - Likewise, election workers should consider work with local first responders to understand their standard operating procedures for various types of emergency calls.
  - Law enforcement and local election workers should consider discussing the procedures to set up a flag or premise alert for their home residence and election locations in their local computer-aided dispatch system (CAD). The premise alert or flag in CAD would inform the responding law enforcement personnel to call a provided phone number to alert them of the dispatch prior to law enforcement's arrival at the location and alert 9-1-1 staff and possible responding officers with a specific note about swatting concerns.

- **Share Critical Information about Election Facilities with First Responders**. Election offices should consider sharing the following information with law enforcement and other emergency management partners and ensure they are aware of the importance of keeping it confidential:
  - The addresses of election-specific locations, including polling places, storage facilities for election and voting system infrastructure, administrative offices, and central count facilities;
  - Critical facility information for these locations, such as floor plans and fire and utility information; and
  - Contact information for critical election staff who can be reached in the event of a possible incident.

- **Establish Communications Protocols and Train for Potential Scenarios.** Election offices and law enforcement should consider:
  - Discussing and exercising potential swatting scenarios amongst key stakeholders so that all parties understand the potential response ahead of time.
  - Establishing communication channels with local, regional, and state election staff to share information about swatting incidents, so if the incident occurs in one jurisdiction others are alerted for the possibility of similar incidents within theirs.
  - Providing election workers and poll workers with swatting and de-escalation training.
  - Providing cybersecurity training to all staff to reinforce individual good practices around protecting personally identifiable information online.
  - Recommending election workers discuss the risk of swatting with other members of their household; plan and practice what to do in the event of a swatting incident at their personal residence.

- **Stay Informed on National Threat Trends.** Law enforcement should consider:
  - Conferring with other local, state, and federal authorities, including the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), on current trends in swatting, as well as indicators of swatting calls.
  - Provide training to personnel, including 9-1-1 dispatchers, on swatting indicators and the potential for swatting related to elections.

- **Reduce Availability of Election Worker Personally Identifiable Information Online**. Election workers should consider:
  - Checking if state law allows for the records of public employees to be omitted from online search databases, and opt into this service, if available.
  - Using services that remove personally identifiable information from the internet.
  - Using strong, unique passwords on all devices and accounts, including smart home devices.
  - Turning on multi-factor authentication (MFA) on all devices and accounts, including smart home devices.
  - Using a virtual private network (VPN) to conceal device IP addresses, and therefore the associated physical location.
  - Being cognizant of what is posted on social media related to individuals' locations.

Swatting Incident Response: What to Do During and After a Swatting Incident

Recommendations for Election Workers on What to Do During a Swatting Incident: In the unfortunate event that your home or place of work is targeted by a swatting attack, stay calm. Listen to and cooperate with law enforcement. While there may be no real emergency, law enforcement is likely unaware of this and may respond to your location with a large law enforcement presence. The following are some considerations to help mitigate risk during an emergency services response to a swatting incident:

- During a law enforcement response, you may be treated like a suspect until the incident is resolved. Law enforcement's priority is to ensure that there is no threat. The situation will likely be very stressful and frustrating for both you and the emergency responders. To resolve the situation quickly, comply with all law enforcement's commands, do not offer any resistance, and answer questions concisely. To ensure your safety, make sure your hands are visible to law enforcement, and make slow and deliberate movements.
- If you suspect you may have been the target of a swatting incident, call 9-1-1. Provide the dispatcher with your name, address, and as many details as possible. Inform them that there is not an emergency at your home or office (as applicable) and be prepared to answer any questions they may have.
- Law enforcement will likely not allow anyone to leave the premises until they have established there is not an actual emergency. Election officials should ensure their Continuity of Operations Plan includes how operations will continue in case of a swatting incident at an election office or other election location—for example, ensuring critical equipment and materials are secure.

Recommendations for Election Workers and Law Enforcement following a Swatting Incident: If a swatting incident occurs, the following recommended actions will help facilitate proper incident reporting and assist with identifying potential risk to other election offices and election workers.

- If election workers believe they, their family, their staff or their office have been the victim of a swatting incident, they should first report this potential crime to local law enforcement and then contact the FBI through the Election Crimes Coordinators at their local field office, submit a tip to 1-800-CALL-FBI (1-800-225-5324), or online at tips.fbi.gov[4].
- If a swatting incident does occur targeting election workers or facilities, encourage state election staff to share information about the incident, so other election jurisdictions are alerted for the possibility of similar incidents. After the incident, election workers can notify CISA at report@cisa.gov or 1-844-Say-CISA (1-844-729-2472) so it can alert other election workers in the event of a larger scale event.
- Swatting incidents may be local events or part of a broader national-level action. Law enforcement should consider immediately reporting these incidents to their local FBI field office.
- Federal, state and local law enforcement can contact the Industry Traceback Group (ITG) to help ascertain the identity of the call originator or gateway provider. The ITG currently serves as the Federal Communications Commission (FCC)-designated traceback consortium under the federal TRACED Act of 2019, and FCC regulations today require that all domestic voice service providers cooperate with the traceback process.[5] Through the traceback process, the ITG obtains information about offending callers as well as voice service providers that carry, originate, and bring into the United States illegal traffic. The ITG routinely obtains this information within a day or two, if not hours, of initiating a traceback, and the process works even if a call is spoofed. Law enforcement can initiate requests for assistance from ITG at: https://tracebacks.org/for-government. It is important to note that due to varying data retention policies across telecommunications providers, the efficacy of this service declines over time, and we recommend initiating traceback requests as soon as possible.

ADDITIONAL RESOURCES

- Committee for Safe and Secure Elections: "Combatting Swatting Attempts." https://safeelections.org/wp-content/uploads/2024/01/Combatting-Swatting-Attempts-CSSE-.pdf

[4] Election Crimes and Security — FBI
[5] About – Industry Traceback Group (tracebacks.org)